UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/760,393	01/21/2004	Ming-Shiang Lai	BHT-3111-403	1300

7590 06/19/2007

BRUCE H. TROXELL
SUITE 1404
5205 LEESBURG PIKE
FALLS CHURCH, VA 22041

EXAMINER	
PALIWAL, YOGESH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/760,393	LAI ET AL.	
	Examiner	Art Unit	
	Yogesh Paliwal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 January 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

2. The drawings are objected to because of following informalities:

- Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).
- Figures 3 and 4 are objected to because "Extract signal", in both figures, is corresponding to numeral 270, however in the specification "Extract signal" is always referred with a reference numeral 274. Applicant is suggested to either change reference numeral for "Extract signal" in Fig. 3 and Fig. 4 to "274" or change reference numeral "274" (referring to "Extract signal") to "270" wherever it has appeared in the specification.
- Figure 4 is objected to because "BD3" in the "Second storage unit (24)" and "format device (275)", should be "BD2".
- Figure 4 is objected to as failing to comply with 37 CFR 1.84(p)(5) because it does not include the following reference sign(s) mentioned in the description of figure 4 (Specification Page 6 paragraph 2 and Page 7 paragraph 1): "27" (Processor, at page 7 line 7).

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities:

- In page 1 line 1, replace "IIEEE" with "IEEE"
- In page 4 line 1, delete "Please refer to fig. 2,"
- In Page 4 line 12, "refer Fig. 3", should read, "refer to Fig. 3"
- In page 5 line 23, "second input of the second storage unit", should read, "second input **from** the second storage unit"

- In page 5 line 26, "processed signal" is referred using numeral "270", however, in figures 3 and 4, "processed signal" is not represented by any drawing numeral, as a result applicant is advised to either add a drawing numeral (different then "270", because "270" is a reference numeral for "extract signal") in figures 3 and 4, or delete "270" from the specification, wherever it is used to refer to "processed signal".
- In page 6 line 35, "format device 274", should read, "format device 275".
- On page 7 line 4, "the D1 and D3 sent by to the", should read, "the D1 and D3 sent by **format device 275** to the".
- On Page 7 line 5, "second storage unit 24 will become BD0, BD1 and BD2", should read, "second storage unit 24 will become BD0 and BD1". [Note: Only bytes D1 and D3 were sent by the format device to the second storage unit and they are both 1 byte long, then how can they "become BD0, BD1 and BD2", which is 3 bytes long space.]

Appropriate correction is required.

Claim Objections

4. Claim 3 is objected to because it includes reference character ("27" for processor), which is not enclosed within parentheses.

Reference characters corresponding to elements recited in the detailed description of the drawings and used in conjunction with the recitation of the same element or group of elements in the claims should be enclosed within parentheses so as to avoid confusion

with other numbers or characters which may appear in the claims. See MPEP § 608.01(m).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1,3,5,6,7,8,9,10,11,12,13,14 and 15 are rejected under 35 U.S.C. 102(e) as being anticipated by Yang et al. (US 7,003,118), hereinafter Yang.

Regarding **Claim 1**, Yang discloses a programmable data processing apparatus, comprising:

a first storage unit **(Fig. 3 Numeral 335, Column 7 lines 9-13)**, which stores auxiliary data needed in a encryption algorithm for data processing **(Column 7, lines 9-13, "...includes the on-chip Tx Security Association Database (SAD) and the host interface")**, wherein, when the encryption algorithm is varied, the auxiliary data stored in the first storage unit can be updated correspondently from outside **(Column 7, lines 9-13, "The host is**

responsible for maintaining the Tc SAD including aging and updating performed via the host interface.");

a reader, coupled to the first storage unit for receiving an index so as to read an auxiliary data from the first storage unit according to the index **(Fig. 3, Numeral 310, column 5, lines 61-66, "Fig. 3 includes an IPSEC TX Packet Parser state machine 310 that scans outboud data packets while they are being downloaded from the host into NIC memory; SA_ID's 316 which is an index into a security association database that stores the encryption key...")**; and

a processor, coupled to the reader for receiving a data signal corresponding to the index so as to process the data signal according to the auxiliary data corresponding to the index **(Fig. 3, numeral 325, column 3, lines 48-51, "...a modifier (Mongooses, for example) configured to modify fields of packets in said input buffer based on the scanned predetermined fields.")**

Regarding **claim 3**, rejection of claim 1 is incorporated and Yang further discloses a third storage unit coupled to the processor, for receiving a processed data signal from the processor, and output the processed signal to a posterior circuit **(Fig. 3, numeral 320, Column 6, lines 66-67 and Column 7, lines 1-3, "The IPSEC Tx Ctrl State Machine 320 then performs context switch (programs the MONGOOSE 325 context/control registers) accordingly. After all these steps are done it enables the IPSEC Tx Data State Machine**

330 to start Ipsec service, i.e. encryption, authentication, or both") when the processed signal is accumulated to a designated amount of bits **(Yang does not explicitly discloses that processed signal is outputted when processed signal is accumulated to a designated amount of bits. However, since the system of Yang can support various encryption algorithms and it is well known that different algorithms use different block sizes for encryption. Therefore, It is implied that processed signal is outputted when processed signal is accumulated to a designated amount of bits as required by the algorithm selected by the system of Yang)**.

Regarding **claims 5-8**, rejection of claim 1 is incorporated and Yang further discloses that the first storage unit is an electrically erasable programmable read only memory (EEPEOM) **(Column 10, lines 33-43, "The storage medium...ROMs, RAMs, EPROMs, EEPROM...")**

Regarding **Claim 9**, the rejection of claim 1 is incorporated and Yang further discloses an initialization device coupled to the reader, which is used for setting partial bits of the data signal to a specified value according to the auxiliary data corresponding to the index **(Fig. 4, numeral 445, Column 7, lines 24-27, "In the case of an authentication protocol, the IPSEC Tx Data state Machine 330 replaces mutable fields in IP header and/or IP header options with zero for ICV computation.")**

Regarding **Claim 10**, the rejection of claim 9 is incorporated and further Yang discloses that the specified value can be one of the following: 0 and 1 **(Fig.**

4, numeral 445, Column 7, lines 24-27, "In the case of an authentication protocol, the IPSEC Tx Data state Machine 330 replaces mutable fields in IP header and/or IP header options with zero for ICV computation.")

Regarding **Claim 11**, the rejection of claim 1 is incorporated and further Yang discloses that a discard device coupled to the reader, which is used for discarding partial bits of the data signal according to the auxiliary data corresponding to the index **(Column 7, lines 24-27, "In the case of an authentication protocol, the IPSEC TX Data State Machine 330 replaces mutable fields in IP header and/or IP header options with zero for ICV computation.")**

Regarding **Claim 12**, the rejection of claim 1 is incorporated and further Yang discloses that a format device **(Fig. 3, numeral 320)** having a first input for inputting data **(Fig. 3 signal coming from numeral 317 and going to numeral 320 can be interpreted as first input)** and a second input for receiving a register signal coming from a second storage unit **(Fig.3, signal coming from numeral 325 and going into numeral 320 can be interpreted as second input)**, wherein the format device will format the first input and the second input according to a process length so as to output a processed signal **(Column 7, lines 2-3, "After all these steps are done, it enables the IPSEC TX Data State Machine 330 to start Ipsec service, i.e. encryption, authentication, or both.")**, moreover, the data exceeding the process length will be send to the second storage unit for registering **(column 6 lines 66-67, "The IPSEC Tx Ctrl**

State Machine 320 then performs context switch (programs the MONGOOSE 325 context/control registers) accordingly")

Regarding **Claim 13**, the rejection of claim 12 is incorporated and further Yang discloses that wherein the second storage unit **(Fig.3, numeral 325, "Context/Control Register Space")** connecting to the format device of the processor **(Fig. 3, numeral 320)** can receive a preload signal and the data exceeding the process length coming from the processor **(Column 6, lines 49-51)**, wherein the forgoing inputted data is registered **(Fig. 3, numeral 325, Column 6 lines 3-9, "an IPSEC Engine Tx Ctrl State Machine 320 uses the FIFO data to look up the Security Association (from the security association database) indicated by the FIFO stored data, and is used to program a programmable device (MONGOOSE 325) which performs the security association and/or ESP processing required on the current outbound data traffic.")**, and the register signal is outputted to the format device of the processor by the second storage unit **(Column 7, lines 2-3, "After all these steps are done, it enables the IPSEC Tx Data State Machine 330 to start Ipsec service, i.e. encryption, authentication, or both.")**

Regarding **Claim 14**, the rejection of claim 13 is incorporated and further Yang discloses that the format device will prioritize the second input coming from the second storage **(Column 7, lines 6-8, "The state machine does not retrieve next entry from the FIFO queue until it receives acknowledgment of Ipsec service completion from IPSEC Tx Data State Machine 330").**

Regarding **Claim 15**, the rejection of claim 13 is incorporated and further Yang discloses that the second storage unit is a register **(Fig. 3, numeral 325, "Context/Control Register Space")**

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yang in view of Applicant's Admitted Prior Art (AAPA).

Regarding **Claim 2**, rejection of claim 1 is incorporated and Yang discloses that any kind of encryption algorithm can be utilize however, he does not explicitly discloses that encryption algorithm is IEEE802.11i Counter-Mode/CBC-MAC Protocol (CCMP), and the data signal is a portion of MAC Service Data Unit (MSDU) of wireless local area network (WLAN).

However, AAPA discloses that using IEEE802.11i Counter-Mode/CBC-MAC Protocol (CCMP) on a portion of MAC Service Data Unit (MSDU) of wireless local area network (WLAN) was well known in the art at the time

applicant's invention was made **(See AAPA, Page 1, paragraph 3 and page 2, paragraph 1)**.

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to use IEEE802.11i Counter-Mode/CBC-MAC protocol (CCMP) as an encryption algorithm as taught by AAPA in the system of Yang *to provide "data encryption and sender authentication" (Yang, Column 1, lines 61-65) in wireless networking.*

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yang in view of Whiting et al. (Whiting, D., Housley, R. and N. Ferguson, "AES Encryption & Authentication Using CTR Mode & CBC-MAC", IEEE P802.11 doc 02/001r2, March 5, 2002), hereinafter Whiting.

Regarding claim **4**, rejection of claim 3 is incorporated and Yang does not disclose that designated amount of bits is 128 bits.

However, Whiting, in the same field of endeavor of secure wireless communication discloses that when CCMP is used the block size of 128 bits is used for AES encryption **(Page 2, Paragraph 2, "CCM is currently only defined for use with block ciphers with a 128-bit block size, such as AES.")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to set the designated amount of bits in the system of Yang to 128 bits as taught by Whiting *to implement AES encryption*

under 802.11i protocol which requires block size of 128 bits (Whiting, Page 2, Paragraph 3).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

YP
6/11/2007